## AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

**Listing of Claims**

1-29. (Cancelled)

30. (New) A method of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of:

said first cryptographic means generating a freshness token;

said first cryptographic means generating said session key based on said shared secret key and said generated freshness token;

providing said session key (K) to said first network element;

providing said freshness token to said second cryptographic means;

said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token; and,

providing said copy of said session key to said second network element.

31. (New) A method of enabling secure communication between a first network element of a first network domain and a second network element of a second network domain, said first network domain comprising first cryptographic means and means for sharing a secret key with said second network domain comprising second cryptographic means, said method comprising the steps of:

said first cryptographic means generating a freshness token;

said first cryptographic means generating said session key based on said shared secret key and said generated freshness token;

providing said session key to said first network element;

providing said freshness token to said second cryptographic means;

said second cryptographic means generating a copy of said session key based on said shared secret key and said provided freshness token;

providing said copy of said session key to said second network element; and,

said first network element and said second network element securely communicating based on said session key and said copy of said session key.

32. (New) The method according to claim 30, wherein said session key providing step comprises the step of securely providing said session key to said first network element and said session key copy providing step comprises the step of securely providing said copy of said session key to said second network element.

33. (New) The method according to claim 30, wherein said freshness token comprises a random challenge and said method further comprises the steps of :

said first cryptographic means generating an expected response based on said shared secret key and said random challenge;

providing said expected response to said first network element;

said second cryptographic means generating a response based on said shared secret key and said provided random challenge;

providing said response to said first network element; and,

said first network element authenticating said second network element based on a comparison between said expected response and said response.

34. (New) The method according to claim 33, wherein said first cryptographic means comprises an Authentication and Key Agreement (AKA) algorithm for generating said random challenge, said expected response and said session key, and said second cryptographic means comprises an AKA algorithm for generating said response and said copy of said session key.

35. (New) The method according to claim 30, further comprising the steps of:

said first network element providing an identifier associated with said second network domain to said first cryptographic means; and,

said second network element providing an identifier associated with said first network domain to said second cryptographic means.

36. (New) The method according to claim 35, wherein said session key and said copy of said session key are generated based on at least one of said identifier associated with said first network domain and said identifier associated with said second network domain.

37. (New) The method according to claim 35, further comprising the steps of:

said first cryptographic means identifying said shared secret key based on said identifier associated with said second network domain; and,

said second cryptographic means identifying said shared secret key based on said identifier associated with said first network domain.

38. (New) The method according to claim 30, wherein said first cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said first network domain and said second cryptographic means is an AAA server provided in a network node of said second network domain.

39. (New) The method according to claim 30, wherein said first network domain shares a second secret key with a third network domain comprising third cryptographic means and at least a third network element.

40. (New) The method according to claim 30, wherein said first network domain is managed by a first communications network operator and said second network domain is managed by a second different communications network operator.

41. (New) The method according to claim 30, further comprising the step of intermittently replacing said shared secret by a new shared secret by basing a key

agreement between said first network domain and said second network domain on said shared secret.

42. (New) A system of establishing a session key shared between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises:

first cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token;

means for providing said session key from said first cryptographic means to said first network element; and,

means for providing said freshness token to said second network domain;

wherein said second network domain comprises:

second cryptographic means for generating a copy of said session key based on said shared secret key and said provided freshness token; and,

means for providing said copy of said session key from said second cryptographic means to said second network element.

43. (New) A system of enabling secure communication between a first network element of a first network domain and a second network element of a second network domain, said first network domain sharing a secret key with said second network domain, wherein said first network domain comprises:

first cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token;

means for providing said session key from said first cryptographic means to said first network element; and,

means for providing said freshness token to said second network domain;

said second network domain comprises:

second cryptographic means for generating a copy of said session key based on said shared secret key and said provided freshness token; and,

means for providing said copy of said session key from said second cryptographic means to said second network element, said first network element comprises means for conducting secure communication with said second network element based said session key and said second network element comprises means for conducting secure communication with said first network element based on said copy of said session key.

44. (New) The system according to claim 42, wherein said session key providing means is adapted for securely providing said session key from said first cryptographic means to said first network element and said session key copy providing means is adapted for securely providing said copy of said session key from said second cryptographic means to said second network element.

45. (New) The system according to claim 42, wherein said freshness token comprises a random challenge and said first cryptographic means comprises means for generating an expected response based on said shared secret key and said random challenge and said second cryptographic means comprises means for generating a response based on said shared secret key and said random challenge, said first network domain comprises means for providing said expected response to said first network element and said second network domain comprises means for providing said response to said first network element, wherein said first network element comprises means for authenticating said second network element based on a comparison between said expected response and said response.

46. (New) The system according to claim 45, wherein said first cryptographic means comprises an Authentication and Key Agreement (AKA) algorithm for generating said random challenge, said expected response and said session key, and said second cryptographic means comprises an AKA algorithm for generating said response and said copy of said session key.

47. (New) The system according to claim 42, wherein said first cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said first network domain and said second cryptographic means is an AAA server provided in a network node of said second network domain.

48. (New) The system according to claim 42, further comprising a third network domain with third cryptographic means and at least a third network element, said first network domain and said third network domain share a second secret key.

49. (New) The system according to claim 42, wherein said first network domain is managed by a first communications network operator and said second network domain is managed by a second different communications network operator.

50. (New) The system according to claim 42, further comprising means for intermittently replacing said shared secret by a new shared secret, said shared secret replacing means is adapted for replacing said shared secret based on a key agreement between said first network domain and said second network domain using said shared secret.

51. (New) A network domain comprising:

a first network element adapted for communication with a second network element of an external network domain, wherein said network domain and said external network domain sharing a secret key;

cryptographic means for generating a freshness token and for generating a session key based on said shared secret key and said generated freshness token;

means for providing said session key from said cryptographic means to said first network element: and,

means for providing said freshness token to said external network domain, wherein said external network domain comprises means for generating a copy of said

session key for said second network element based on said shared secret key and said provided freshness token.

52. (New) The network domain according to claim 51, wherein said session key providing means is adapted for securely providing said session key from said cryptographic means to said first network element.

53. (New) The network domain according to claim 51, wherein said freshness token comprises a random challenge and said cryptographic means comprises means for generating an expected response based on said shared secret key and said random challenge and said external network domain comprises means for generating a response based on said shared secret key and said random challenge, said network domain comprises means for providing said expected response to said first network element and said external network domain comprises means for providing said response to said first network element, wherein said first network element comprises means for authenticating said second network element based on a comparison between said expected response and said response.

54. (New) The network domain according to claim 51, wherein said cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said network domain.

55. (New) A network domain comprising:

a first network element adapted for communication with a second network element of an external network domain, wherein said network domain and said external network domain sharing a secret key;

cryptographic means for generating a session key based on said shared secret key and a freshness token provided from said external network domain; and,

means for providing said session key from said cryptographic means to said first network element, wherein said external network domain comprises means for generating said freshness token and for generating a copy of said session key for said

second network element based on said shared secret key and said generated freshness token.

56. (New) The network domain according to claim 55, wherein said session key providing means is adapted for securely providing said session key from said cryptographic means to said first network element.

57. (New) The network domain according to claim 55, wherein said freshness token comprises a random challenge and said cryptographic means comprises means for generating a response based on said shared secret key and said random challenge and said external network domain comprises means for generating an expected response based on said shared secret key and said random challenge and means for providing said expected response to said second network element, said network domain comprises means for providing said response to said second network element, wherein said response and said expected response enables said second network element to authenticate said first network element.

58. (New) The network domain according to claim 55, wherein said cryptographic means is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said network domain.

* * *